DIVISIBILITY OF FIBONOMIALS AND LUCASNOMIALS VIA A GENERAL KUMMER RULE

CHRISTIAN BALLOT

ABSTRACT. Marques et al. have recently studied some specific Fibonomial divisibility questions. For instance, they determined all integers $n \geq 1$ such that the Fibonomial $\binom{3n}{n}_F$ is divisible by 3. We reexamine those questions with the Kummer-like rule established by Knuth and Wilf for Fibonomials. After stating a Kummer result valid for all primes and Lucasnomials, i.e., generalized binomials $\binom{*}{*}_U$ with U a fundamental Lucas sequence, we obtain broad divisibility theorems for Lucasnomials along the line of Marques et al. original questions.

1. INTRODUCTION

In the papers [5, 6], one finds three divisibility theorems and a conjecture concerning Fibonomial coefficients. We state them below.

Theorem 1.1. *Given an integer $n \geq 1$, we have*

$$3 \text{ divides } \binom{3n}{n}_F \iff n \geq 3 \text{ and } n \neq 2 \cdot 3^r, \ (r \geq 1).$$

Theorem 1.2. *Let s be a positive integer. Then*

$$3 \text{ divides } \binom{sn}{n}_F \text{ for all } n \geq 1 \iff 12 \text{ divides } s.$$

Theorem 1.3. *Let p be a prime congruent to $\pm 2 \pmod 5$. Then for all integers $a \geq 1$*

$$p \text{ divides } \binom{p^{a+1}}{p^a}_F.$$

Conjecture 1.4. *Let p be a prime congruent to $\pm 1 \pmod 5$. Then for all integers $a \geq 1$*

$$p \text{ does not divide } \binom{p^{a+1}}{p^a}_F.$$

Corresponding results for ordinary binomials are easy to establish and rather plain in comparison. Indeed, we have the following propositions.

Proposition 1.5. *Given a prime p, we have*

$$p \text{ divides } \binom{pn}{n} \text{ for all integers } n \geq 1.$$

Proposition 1.6. *Let s be a positive integer and p be a prime. Then*

$$p \text{ divides } \binom{sn}{n} \text{ for all integers } n \geq 1 \iff p \text{ divides } s.$$

If $(X_n)_{n\geq 0}$ is a sequence of integers, where $X_0 = 0$ and $X_n \neq 0$ for $n \geq 1$, we define for all nonnegative integers m and n the generalized binomials with respect to X as

$$\binom{m}{n}_X = \begin{cases} \frac{X_m X_{m-1} \cdots X_{m-n+1}}{X_n X_{n-1} \cdots X_1}, & m \geq n \geq 1; \\ 1, & n = 0; \\ 0, & \text{otherwise.} \end{cases}$$

Fibonomials are generalized binomials with respect to the Fibonacci sequence $X = F$. They are known to be integers. The p-adic valuation of an integer m, denoted by $\nu_p(m)$, is the largest exponent e such that p^e divides m. The proofs of the three theorems given in [5] and [6] consisted in comparing the 3-adic or the p-adic valuations of both the numerator and the denominator of the Fibonomial coefficient at hand. If their difference is strictly positive then the prime divides the coefficient. The ingredients were the well-known regularity with which the powers of a prime enter the Fibonacci sequence, the Legendre p-adic valuation of a factorial together with upper and lower estimates for this Legendre formula. They do not use the generalizations of Kummer's result on the p-adic valuation of binomials which would have seemed natural in this context.

Kummer [4, p. 116], showed that the p-adic valuation of a binomial coefficient $\binom{m+n}{n}$ is equal to the number of carries that occur when one adds m and n in base-p notation. A generalization of this classical result was established in [3] for certain sequences of positive integers which, besides the sequence of natural numbers, include the Fibonacci sequence. Knuth and Wilf did state their generalized Kummer result for the particular case of the Fibonacci sequence.

Theorem 1.7. *Let m and n be two positive integers. Let p be a prime of rank ρ in the Fibonacci sequence. If p is odd, then the p-adic valuation of the Fibonomial coefficient $\binom{m+n}{n}_F$ is equal to the number of carries that occur to the left of the radix point when m/ρ and n/ρ are added in base-p notation, plus $\nu_p(F_\rho)$ if a carry occurs across the radix point. If p is 2, then one counts the above carries and adds one in case there is a carry from the first to the second digit to the left of the radix point.*

If P and Q are any two integers, Q nonzero, then the fundamental Lucas sequence $U = U(P, Q)$ with parameters P and Q is defined by $U_0 = 0$, $U_1 = 1$ and, for all $n \geq 0$, recursively by $U_{n+2} = PU_{n+1} - QU_n$. Any prime p, $p \nmid Q$, possesses a rank of appearance ρ in U which is the least positive t such that p divides U_t. The law of appearance for primes says that, for p odd, ρ divides $p - \epsilon_p$, where $\epsilon_p = (D \mid p)$, $(- \mid -)$ denoting the Legendre character, and $D = P^2 - 4Q$, while, for $p = 2$, $\rho = 2$, if $2 \mid D$, and $\rho = 3$, if $2 \nmid D$. It is well-known that p divides U_n if and only if ρ divides n. If $U_2U_3U_4U_6 \neq 0$, then the sequence U is said to be *nondegenerate*. In that case, $U_n \neq 0$ for all $n > 0$. We may then consider Lucasnomials, i.e., generalized binomials with respect to U. When $(P, Q) = (2, 1)$, then $U_n = n$ for all $n \geq 0$; the corresponding Lucasnomials are the ordinary binomials. If $(P, Q) = (1, -1)$, then $U = F$, the Fibonacci sequence and we get the oft-studied Fibonomial coefficients. To each $U(P, Q)$ is associated a *companion* Lucas sequence V which satisfies the same recursion as the U sequence, but has initial values $V_0 = 2$ and $V_1 = P$. We recall that any fundamental Lucas sequence U is a divisibility sequence, that is, $m \mid n$ implies $U_m \mid U_n$. Lucasnomials with respect to a nondegenerate U are well-known to be integers, and in some reasonable sense, it is true of Lucasnomials with respect to a degenerate U as well [1, Appendix].

Although it is clear that the authors of the two papers [5] and [6] have opened a new vein of investigations in raising these few divisibility questions, that is, there are many similar questions that may be asked, we will stay on their tracks only broadening somewhat their

questions. Thus, given a fundamental nondegenerate Lucas sequence U and a prime p, we are interested in the three questions.

Question 1. What can be said of the set of integers $n \geq 1$ such that $p \mid \binom{pn}{n}_U$?

Question 2. Can one find a simple necessary and sufficient condition on $s \geq 1$ such that p divides $\binom{sn}{n}_U$ for all $n \geq 1$?

Question 3. Given $b > a \geq 0$, what is the p-adic valuation of $\binom{p^b}{p^a}_U$?

The paper contains six sections besides this introduction. In Sections 2 and 3 we stay with the Fibonacci sequence. In Section 2 we use Theorem 1.7 to prove Conjecture 1.4 and reprove Theorem 1.1. Indeed, the proof of Theorem 1.1 in [5] was divided into four propositions and took four pages. Proposition 9, the last of these four propositions, only treated – for the sake of brevity and illustration – one among forty-eight cases, thus leaving forty-seven cases to the patience or the good faith of the readers. We present a fully explicit, short proof of Theorem 1.1 that makes the exceptional integers of the form $2 \cdot 3^r$ appear naturally. In Section 3 we tackle Question 1 for $p = 2, 5$ and 7, before giving an upper estimate on the size of the set of exceptional integers n for which $p \nmid \binom{pn}{n}_F$. To go further we establish in Section 4, after Knuth and Wilf, a Kummer-like theorem that applies to all nondegenerate fundamental Lucas sequences and all primes p. In Sections 5, 6, and 7, we put to use the Kummerian tool of Section 4 to respectively make progress on Question 1 and fully answer Questions 2 and 3.

Notation. Note that when adding two nonnegative rational numbers x and y in base p a carry occurs across the radix point if and only if the sum of the fractional parts of x and y is at least 1, i.e., if and only if $\{x\} + \{y\} \geq 1$. In such an addition (or a subtraction), because of Theorem 1.7, we will say that a carry is *relevant* if and only if it occurs either across, or to the left of the radix point. We define the boolean function $c_p(x, y)$, or $c(x, y)$, to be 1 if and only if there is at least one relevant carry in the addition of x and y in base p.

2. Fibonomial Divisibility with the Rescue of Theorem 1.7

We begin by mutating Conjecture 1.4 into a theorem.

Theorem 2.1. *Let p be a prime congruent to $\pm 1 \pmod 5$. Then for all integers $a \geq 1$*

$$p \text{ does not divide } \binom{p^{a+1}}{p^a}_F.$$

Proof. By Theorem 1.7, p does not divide $\binom{p^{a+1}}{p^a}_F$ if and only if $c_p(p^a/\rho, \sigma p^a) = 0$, where $\sigma = (p-1)/\rho$. Since $1 \leq \sigma < p$, the base-p expansion of the integer σp^a has leading digit σ at the $(a+1)$st position to the left of the radix point followed by only 0's. The rational number p^a/ρ, less than p^a, has all its p-ary digits to the right of this $(a+1)$st position. Thus, there are no carries in the addition of p^a/ρ to σp^a in base p and therefore no relevant ones. □

Lemma 2.2. *Let p be a prime and $\ell \geq 1$ an integer. The addition of ℓ and $(p-1)\ell$ in base p produces at least one carry.*

Proof. We have $\binom{p\ell}{\ell} = p \times \binom{p\ell-1}{\ell-1}$. Since p divides the binomial $\binom{p\ell}{\ell}$, there is a carry in our addition by Kummer's Theorem. However, one can also give a direct proof. If d is the least significant nonzero digit of ℓ expressed in base p, then $p - d$ is the least significant nonzero digit of $(p-1)\ell$ and occupies the same position. Thus, there is a carry in the addition. □

We now give a proof of Theorem 1.1 based on Knuth and Wilf's Kummer-like result.

Proof. The rank of $p = 3$ in the Fibonacci sequence is 4. Put $x = n/4$ and $y = 2n/4$. By Theorem 1.7, $3 \mid \binom{3n}{n}_F$ if and only if $c(x, y) = 1$. If $4 \mid n$, then x and y are integers and $c(x, y) = c(x, 2x) = 1$ by Lemma 2.2. If $n = 3 + 4k$, then $2n = 2 + 4(2k + 1)$. The sum of the fractional parts of x and y exceeds 1, so there is a carry across the radix point. If $n = 1 + 4k$, then $2n = 2 + 8k$. Thus, $c(x, y) = c(k, 2k) = 1$, by Lemma 2.2, unless $k = 0$ and $n = 1$. If $n = 2+4k$, then $2n = 4(2k+1)$. Hence, $c(x, y) = c(k, 2k+1)$. We organize the discussion according to the value of $k \pmod 3$. If $3 \mid k$, then $c(k, 2k + 1) = c(k, 2k) = 1$, unless $k = 0$ and $n = 2$. If $k = 2+3k_1$, then $2k+1 = 2+3(2k_1+1)$. The least significant digits in k and $2k+1$ being both 2, there is a carry. Finally if $k = 1 + 3k_1$ we find that $c(x, y) = c(k, 2k + 1) = c(k_1, 2k_1 + 1)$. Thus, reiterating our reasoning, we see that $c(x, y) = 0$ if and only if there is an $r \geq 0$ and an rth integer $k_r = 1$ with $k = 1 + 3(1 + 3(1 + \cdots + 3(1 + 3k_r)) \cdots) = 1 + 3 + 9 + \cdots + 3^r$, i.e., if and only if $n = 2 + 4k = 2 \cdot 3^{r+1}$. □

3. Can we Generalize Theorem 1.1 to Other Primes?

The analogue of Theorem 1.1 for the prime 2 is an easy result.

Theorem 3.1. *For $n \geq 1$ an integer, we have*

$$2 \text{ divides } \binom{2n}{n}_F \iff n \geq 2.$$

Proof. Note that, by Theorem 1.7, 2 divides $\binom{2n}{n}_F$ if and only if $c_2(n/3, n/3) = 1$. Write $n = 3k + \nu$, $0 \leq \nu \leq 2$. Clearly $c_2(n/3, n/3) \geq c_2(k, k)$. But, by Lemma 2.2, $c_2(k, k) = 1$ for all $k \geq 1$. If $k = 0$, then $n = 1$ or 2 and there is a carry across the radix point if and only if $n/3 + n/3 \geq 1$, i.e., if and only if $n = 2$. □

With the help of Theorem 1.7, the determination of the integers n for which p divides $\binom{pn}{n}_F$ when p is 2 or 3 was simple. But how easy is it to settle the analogous divisibility questions for primes larger than 3?

The case of $p = 5$ is unique because $\nu_5(F_n) = \nu_5(n)$ for all $n \geq 0$ so that the 5-adic valuation of the Fibonomial $\binom{m+n}{n}_F$ is the same as that of the binomial $\binom{m+n}{n}$. Therefore the answer is given by Proposition 1.5. Hence, 5 divides $\binom{5n}{n}_F$ for all $n \geq 1$.

Can we determine those integers $n \geq 1$ for which 7 divides $\binom{7n}{n}_F$?

Note that $\rho_F(7) = 8$. Putting $x = n/8$, 7 will divide $\binom{7n}{n}_F$ if and only if $c_7(x, 6x) = 1$, by Theorem 1.7. Set $n = \eta + 8k$, where $0 \leq \eta \leq 7$. We break the investigation into lemmas.

Lemma 3.2. *We have*

$$c_7(x, 6x) = \begin{cases} 1, & \text{if } \eta = 0, 1, 5, 6 \text{ or } 7; \\ c_7(k, \eta - 1 + 6k), & \text{otherwise.} \end{cases}$$

Proof. If $\eta = 0$, then $c_7(x, 6x) = c_7(k, 6k) = 1$, by Lemma 2.2. If $\eta = 1$, then $6n = 6+48k$. The sum of the fractional parts of x and $6x$ being less than 1, we find that $c_7(x, 6x) = c_7(k, 6k) = 1$. If $\eta = 7$, then $6n = 2 + 8(6k + 5)$. Hence, $\{x\} + \{6x\} = (7 + 2)/8 > 1$ and $c_7(x, 6x) = 1$. Similarly, if $5 \leq \eta \leq 6$, then $6n = 8\eta - 2\eta + 48k = (16 - 2\eta) + 8(6k + \eta - 2)$. As $4 \leq 16 - 2\eta \leq 6$ the sum of the fractional parts of x and $6x$ is larger than one and $c_7(x, 6x) = 1$.

If $2 \leq \eta \leq 4$, then $6n = (8 - 2\eta) + 8[(\eta - 1) + 6k]$. Because $\eta + (8 - 2\eta) < 8$, the sum $\{x\} + \{6x\} < 1$ and thus, $c_7(x, 6x) = c_7(k, \eta - 1 + 6k)$. □

Lemma 3.3. *If $n = 2 + 8k$, then $c_7(x, 6x) = 0$ if and only if $k = 1 + 7 + \cdots + 7^\lambda$, for some $\lambda \geq 0$.*

Proof. By Lemma 3.2, $c_7(x, 6x) = c_7(k, 1 + 6k)$. Let κ be the least nonnegative residue of k (mod 7), that is, $k = \kappa + 7k_1$, $k_1 \geq 0$, $\kappa < 7$. If $2 \leq \kappa \leq 6$, then $6k+1 = (8-\kappa)+7(\kappa-1+6k_1)$. But $\kappa + (8 - \kappa) \geq 7$ so $c_7(k, 1 + 6k) = 1$. If $\kappa = 0$, then $c_7(k, 1 + 6k) = c_7(k, 6k) = 1$ by Lemma 2.2. If $k = 1 + 7k_1$, then $1 + 6k = 7(1 + 6k_1)$. Thus, $c_7(k, 1 + 6k) = c_7(k_1, 1 + 6k_1)$. Therefore, $c_7(k, 1+6k) = 0$ implies either $k = 1$ or there exist $k_1, \ldots, k_\lambda$ with $k_\lambda = 1$ such that $k = 1+7k_1 = 1+7(1+7k_2) = \cdots = 1+7(1+7(1+\cdots+7(1+7k_\lambda))\cdots) = 1+7+7^2+\cdots+7^\lambda$. Conversely, if $k = 1 + 7 + 7^2 + \cdots + 7^\lambda$, then $1 + 6k = 7^{\lambda+1}$ and $c_7(k, 1 + 6k) = 0$. □

Lemma 3.4. *If $n = 3 + 8k$, then $c_7(x, 6x) = 0$ if and only if k is of the form*

$$2 \cdot \frac{7^\lambda - 1}{6} + 7^\lambda \cdot \frac{7^\mu - 1}{6}, \text{ for some } \lambda \geq 0,\ \mu \geq 0.$$

Proof. By Lemma 3.2, $c_7(x, 6x) = c_7(k, 2 + 6k)$. Let $k > 0$. Writing $k = \kappa + 7k_1$, $(0 \leq \kappa \leq 6)$, we are about to see that $c_7(k, 2 + 6k) = 0 \implies \kappa = 1$ or 2. Indeed, if $7 \mid k$ or $3 \leq \kappa \leq 6$, then $k \geq 3$ and $\binom{7k+2}{k} = \frac{(7k+2)(7k+1)(7k)}{k(k-1)(k-2)}\binom{7k-1}{k-3}$ is divisible by 7. Hence, by Kummer's rule, $c_7(k, 6k + 2) = 1$. On the one hand, if $k = 1 + 7k_1$, then $2 + 6k = 1 + 7(1 + 6k_1)$. Hence, $c_7(k, 2 + 6k) = c_7(k_1, 1 + 6k_1)$. By the proof of Lemma 3.3, we know, using a base-7 writing, that $k_1 = 11\cdots1_7$ (with, say, μ ones, $\mu \geq 0$) in order for $c_7(k_1, 1 + 6k_1)$ to be 0. Thus, $k = 1 + 7k_1 = 11\cdots1_7$ (with $\mu + 1$ ones). On the other hand, if $k = 2 + 7k_1$, then $2 + 6k = 7(2 + 6k_1)$. Hence, $c_7(k, 2 + 6k) = c_7(k_1, 2 + 6k_1)$. Therefore, since after any string of 2's we may bifurcate to a string of 1's, $c_7(x, 6x) = 0$ if and only if k is of the form $1\cdots12\cdots2_7$ with, say λ 2's and μ 1's. That is, if and only if, k is of the form indicated in the statement of the lemma. Note that if k is of this form, then $6k + 2 = 7^\lambda + 7^{\lambda+\mu}$ explaining the 'if' part of the above 'if and only if' statement. □

Lemma 3.5. *If $n = 4 + 8k$, then $c_7(x, 6x) = 0$ if and only if k is of the form*

$$3 \cdot \frac{7^\lambda - 1}{6} + 7^\lambda \cdot 2 \cdot \frac{7^\mu - 1}{6} + 7^{\lambda+\mu}\frac{7^\nu - 1}{6}, \text{ for some } \lambda \geq 0,\ \mu \geq 0 \text{ and } \nu \geq 0.$$

Proof. By Lemma 3.2, $c_7(x, 6x) = c_7(k, 3 + 6k)$. Let d_i, $i \geq 0$, be the $(i + 1)$-rightmost base-7 digit of k, $k_0 := d_0$ and recursively $k_{i+1} := (k_i - d_i)/7$. Assume $k > 0$. If $d_0 = 0$, then $c_7(k, 3 + 6k) = c_7(k_1, 6k_1) = 1$. If $4 \leq d_0 \leq 6$, then $3 + 6k = (10 - d_0) + 7(d_0 - 1 + 6k_1)$. As d_0 and $10 - d_0$ both belong to $\{4, 5, 6\}$ there is a carry between the first and second digits when adding k to $3 + 6k$. If $d_0 = 1$, then $3 + 6k = 2 + 7(1 + 6k_1)$ and $c_7(k, 3 + 6k) = c_7(k_1, 1 + 6k_1)$, which we know from the proof of Lemma 3.3 to be 0 if and only if $k_1 = (7^l - 1)/6$ for some $l \geq 0$. That is, taking the case $k = 0$ into account, when k is of the form $(7^\lambda - 1)/6$ for some $\lambda \geq 0$. If $d_0 = 2$, then $3 + 6k = 1 + 7(2 + 6k_1)$. Hence, $c_7(k, 3 + 6k) = c_7(k_1, 2 + 6k_1)$. But in that case, by the proof of Lemma 3.4, we know that $c_7(x, 6x) = 0$ if and only if $d_i = 2$ for $0 \leq i < \lambda$ and $d_i = 1$ for $i \geq \lambda$, for some $\lambda \geq 0$. If $d_0 = 3$, then $3 + 6k = 7(3 + 6k_1)$. Hence, $c_7(k, 3 + 6k) = c_7(k_1, 3 + 6k_1)$. So in order to have $c_7(x, 6x) = 0$ and, moving right to left through the base-7 digits of k, we must have a sequence of 3's, followed by a sequence of digits all 2's, followed by a sequence of 1's, where each sequence may potentially be empty. For all such k's, we do have $c_7(k, 3 + 6k) = 0$ because $6k + 3$ is of the form $7^\lambda + 7^{\lambda+\mu} + 7^{\lambda+\mu+\nu}$ for some nonnegative exponents λ, μ and ν. Such numbers have base-7 digits at most 3. □

So we obtain the theorem.

Theorem 3.6. *Given an integer $n \geq 1$, 7 divides $\binom{7n}{n}_F$ unless $n = 1$ or is of one of the forms*

$$2 + 8 \cdot \tfrac{7^\lambda - 1}{6}, \quad (\lambda \geq 0)$$

$$3 + 8 \cdot \left[2 \cdot \tfrac{7^\lambda - 1}{6} + 7^\lambda \cdot \tfrac{7^\mu - 1}{6} \right], \quad (\lambda \geq 0,\ \mu \geq 0)$$

$$4 + 8 \cdot \left[3 \cdot \tfrac{7^\lambda - 1}{6} + 7^\lambda \cdot 2 \cdot \tfrac{7^\mu - 1}{6} + 7^{\lambda+\mu} \cdot \tfrac{7^\nu - 1}{6} \right], \quad (\lambda \geq 0,\ \mu \geq 0,\ \nu \geq 0).$$

It seems that, given a prime p and time, the method might yield explicitly the set E_p of integers n such that $p \nmid \binom{pn}{n}_F$. Instead we use the experience of the primes 3 and 7 to derive a general upper estimate for the size of E_p, which is always a slim set of integers. Let $E_p(x)$ denote the cardinality of $E_p \cap [1, x]$. From Theorems 1.1 and 3.6 we can see that $E_3(x)$ is $O(\log x)$ and $E_7(x)$ is $O(\log^3 x)$. We begin by a general lemma.

Lemma 3.7. *Let $k = d_1 + pk_1 \geq 1$, where $k_1 \geq 0$ is an integer, p is a prime and $0 \leq d_1 < p$. Suppose $c_p(k, d + (p-1)k) = 0$, where $1 \leq d \leq p - 2$. Then $c_p(k_1, d_1 + (p-1)k_1) = 0$ and $1 \leq d_1 \leq d$.*

Proof. If $k_1 = 0$, then the lemma clearly holds. Assume $k_1 \geq 1$. In particular, $k \geq p > d$. If $d_1 = 0$ or if $d_1 > d$ then

$$\binom{d + pk}{k} = \frac{(d + pk) \cdots (pk)}{k(k-1) \cdots (k-d)} \binom{pk - 1}{k - d - 1} \quad \text{is divisible by } p,$$

which, by Kummer's rule, says that $c_p(k, d + (p-1)k) = 1$, a contradiction. Now

$$\begin{aligned} d + (p-1)k &= d + (p-1)(d_1 + k_1 p) \\ &= d - d_1 + p(d_1 + k_1(p-1)). \end{aligned}$$

Thus, as the sum of the least significant p-ary digits of k and $d + (p-1)k$ is $d < p$, we find that $c_p(k, d + (p-1)k) = c_p(k_1, d_1 + (p-1)k_1) = 0$. □

Suppose n belongs to E_p. Write $n = \eta + k\rho$, where k is nonnegative and $1 \leq \eta < \rho$. Note that $\eta \neq 0$ by Lemma 2.2. In fact, more generally η must be *admissible*, i.e., it must satisfy $\frac{\eta}{\rho} + \left\{ \frac{(p-1)\eta}{\rho} \right\} < 1$. Define $s = s_p$ as the largest integer $\left\lfloor \frac{(p-1)\eta}{\rho} \right\rfloor$ over all admissible η's and note that $s \leq p - 2$ as $\eta/\rho < 1$.

Theorem 3.8. *Let p be a prime. Then $E_p(x)$, the number of integers $n \leq x$ such that p does not divide $\binom{pn}{n}_F$, is $O(\log^s x)$, where the implied constant may depend on p, and where the integer s, $0 \leq s \leq p - 2$, was defined above.*

Proof. Let x be large. Assume p has rank ρ. Fix an admissible η. Suppose $n \in E_p$, $n \leq x$ and $n = \eta + k\rho$. To prove our theorem it will suffice to show that the number of k's, $k \leq x$ and $c_p(k, d + (p-1)k) = 0$, is $O(\log^s x)$, where $d = \left\lfloor \frac{(p-1)\eta}{\rho} \right\rfloor$. Indeed, $c_p(n/\rho, n(p-1)/\rho) = c_p(k, d + (p-1)k)$. By Lemma 3.7, d_1, the least significant p-ary digit of k, satisfies $1 \leq d_1 \leq d$, which means the p-ary expansion of k may contain a string of least significant digits all equal to d_1, (possibly) followed by a string of a digit strictly less than d_1, and so forth with possibly more strings of smaller digits. That is in p-ary notation

$$k = 0 \cdots 0 d_u \cdots d_u d_v \cdots d_v \cdots d_w \cdots d_w d_1 \cdots d_1,$$

where $d \geq d_1 > d_w > \cdots > d_v > d_u \geq 1$ and the 0's have been added so as to have all the $1 + \lfloor \log_p x \rfloor$ least significant digits of any $k \leq x$. Let $1 \leq q \leq d$. Choose q digits among the

d possible ones and then 'separate' those $q+1$ digits (including the 0's) by choosing q places among at most $\lfloor \log_p x \rfloor$. There are at most p choices for an admissible η. Hence,

$$\begin{aligned} E_p(x) &\le p \times \sum_{q=1}^{d} \binom{d}{q} \binom{\lfloor \log_p x \rfloor}{q} \\ &\le p \binom{d}{\lfloor d/2 \rfloor} \sum_{q=1}^{d} \binom{\lfloor \log_p x \rfloor}{q} \\ &\le p \binom{s}{\lfloor s/2 \rfloor} s \binom{\lfloor \log_p x \rfloor}{s} = O\big(\log^s x\big). \end{aligned}$$

□

4. A Kummer Theorem Tailored to Fundamental Lucas Sequences

Knuth and Wilf [3] considered a sequence of positive integers $(C_n)_{n\ge 1}$ and showed that

$$\nu_p \binom{m+n}{n}_C = \sum_{k\ge 1} \big(d_{p^k}(m+n) - d_{p^k}(m) - d_{p^k}(n) \big), \tag{4.1}$$

where $d_{p^k}(m)$ is the number of integers i, $1 \le i \le m$, such that p^k divides C_i. This is based on the fact that $\nu_p(C_m C_{m-1} \cdots C_1) = \sum_{k\ge 1} d_{p^k}(m)$, a formula which extends the Legendre formula $\nu_p(n!) = \sum_{k\ge 1} \lfloor \frac{m}{p^k} \rfloor$.

For an easy calculation of $d_{p^k}(m)$ it is convenient that C be a strong divisibility sequence, i.e., that for all positive integers m and n,

$$\gcd(C_m, C_n) = C_{\gcd(m,n)}. \tag{4.2}$$

Indeed, C is strongly divisible if and only if C is *regularly divisible*, which means that for all $m \ge 1$, either m never divides any term C_n, $n \ge 1$, or there exists a $\rho = \rho(m) \ge 1$ such that $m \mid C_n$ if and only if $\rho \mid n$. The integer $\rho(m)$ is called the rank of appearance of m in C. The connection between strong and regular divisibilities was first found by Ward [7]. Hence, if $\rho(p^k)$ exists for all $k \ge 1$, then $d_{p^k}(m) = \lfloor \frac{m}{\rho(p^k)} \rfloor$. In order to have a simple generalization of the rule of Kummer, which we mentioned in the introduction, it is convenient for a regularly divisible sequence to generally satisfy, in addition,

$$\rho(p^{k+1}) = p \cdot \rho(p^k). \tag{4.3}$$

We have a couple of remarks. First the analysis made in [3] for sequences of positive integers is actually valid for all sequences of nonzero integers. All nondegenerate fundamental Lucas sequences $U(P,Q)$ have nonzero terms U_n for all $n \ge 1$. Secondly, although these Lucas sequences are often studied with the hypothesis that $\gcd(P,Q) = 1$, which makes them strong divisibility sequences (here condition (4.2) is replaced by $\gcd(C_m, C_n) = |C_{\gcd(m,n)}|$), strong divisibility is not necessary. Indeed, if $\gcd(P,Q) > 1$, then $U(P,Q)$ nearly remains regularly divisible. That is, regular divisibility holds for all integers m having no *special* prime factors. Special primes are the prime divisors of $\gcd(P,Q)$. Moreover, it was shown in Theorem 3.8, [2, p. 26], that, even when $\gcd(P,Q) > 1$, for all nondegenerate $U(P,Q)$ and all odd primes not dividing Q, we have for $n \ge 1$ an integer

$$\nu_p(U_n) = a + b, \quad \text{if and only if,} \quad n = \lambda p^b \rho, \tag{4.4}$$

where ρ is the rank of p, $\nu_p(U_\rho) = a \ge 1$ and λ is a positive integer prime to p.

Therefore, for all odd primes p not dividing Q and all $k \geq a$, (4.3) holds. Consequently, for such primes, we may determine the p-adic valuation of $\binom{m+n}{n}_U$ using a Kummer-like rule. Indeed,

$$d_{p^k}(m) = \left\lfloor \frac{m}{\rho(p^k)} \right\rfloor = \begin{cases} \lfloor \frac{m}{\rho} \rfloor, & \text{if } 1 \leq k \leq a; \\ \lfloor \frac{m}{p^{k-a}\rho} \rfloor, & \text{if } k > a. \end{cases}$$

As $\lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor = 1$ if and only if $\{x\}+\{y\} \geq 1$, we find that $d_{p^k}(m+n) - d_{p^k}(m) - d_{p^k}(n) = 1$ if and only if there is a carry either across the radix point if $1 \leq k \leq a$, or at position $k-a$ to the left of the radix point if $k > a$ when adding m/ρ and n/ρ in base p.

Theorem 3.30 of [2] gave the 2-adic valuation of all terms of a companion Lucas sequence $V_n(P,Q)$ when Q is odd. Using this together with the identities $U_{3(n+2)} = V_3 U_{3(n+1)} - Q^3 U_{3n}$ and $U_{2n} = U_n V_n$ and an induction on $j = \nu_2(n) \geq 0$, one can get a result comparable to (4.4), but for the prime 2, namely we have the following theorem.

Theorem 4.1. *Suppose $U = U(P,Q)$ is a nondegenerate fundamental Lucas sequence with Q odd. The rank ρ of 2 is either 2, if P is even, or 3, if P is odd. The 2-adic valuation of a term U_n is determined by the fact that 2 divides U_n if and only if ρ divides n, and by the formulas*

$$\nu_2(U_{\rho n}) = \nu_2(U_\rho) + \nu_2(n), \text{ if } P \text{ is even, or if } P \text{ is odd and } Q \equiv 1 \pmod 4,$$

and

$$\begin{cases} \nu_2(U_{3(2n+1)}) = \nu_2(U_3) = 1, \\ \nu_2(U_{6n}) = \nu_2(U_6) + \nu_2(n) = 1 + \nu_2(P^2 - 3Q) + \nu_2(n), \end{cases} \text{if } P \text{ is odd and } Q \equiv -1 \pmod 4.$$

We sum up our remarks in Theorem 4.2, which is a Kummer-like theorem for generalized binomials related to a nondegenerate fundamental Lucas sequence.

Theorem 4.2. *Let $U = U(P,Q)$ be a nondegenerate fundamental Lucas sequence. Let p be a prime not dividing Q of rank ρ in U. Then the p-adic valuation of the Lucasnomial $\binom{m+n}{n}_U$ is equal to the number of carries that occur to the left of the radix point when m/ρ and n/ρ are added in base-p notation, plus $\nu_p(U_\rho)$ if a carry occurs across the radix point, unless p is 2, P is odd and Q is -1 modulo 4, in which case one must add the 2-adic valuation of $(P^2-3Q)/2$ to the previous count if, in the same addition, there is a carry from the first to the second digit to the left of the radix point.*

It might be worth giving an explicit statement for the 2-adic valuation of Lucasnomials.

Corollary 4.3. *Let $U = U(P,Q)$ be a nondegenerate fundamental Lucas sequence with Q odd. Then*

$$\nu_2 \binom{m+n}{n}_U = \begin{cases} C(m,n) + \nu_2(P/2) \cdot c_0, & \text{if } P \text{ is even;} \\ C(m/3, n/3) + \nu_2(P^2 - Q) \cdot c_{-1}, & \text{if } P \text{ is odd and } Q \equiv 1 \pmod 4; \\ C(m/3, n/3) + \nu_2\big((P^2 - 3Q)/2\big) \cdot c_0 + c_{-1}, & \text{if } P \text{ is odd and } Q \equiv 3 \pmod 4, \end{cases}$$

where $C(x,y)$ is the number of carries that occur to the left of the radix point when adding x and y in base 2, and c_i is 1 or 0 according to respectively the presence or the absence of a carry going from position i to $i+1$, and the 0 and -1 positions are respectively the first to the left and the first to the right of the radix point.

Remark. In the above corollary, when P is even, $c_0 = 1$ if and only if m and n are both odd.

5. A Few More Results Concerning Question 1

The results of the previous section make it plain that the proof of Theorem 3.8 holds for all fundamental Lucas sequences. Given U and p, define $E_{U,\,p}$ as the set of integers $n \geq 1$ such that $p \nmid \binom{pn}{n}_U$ and $E_{U,\,p}(x)$ as the cardinality of the set of integers $n \leq x$ in $E_{U,\,p}$.

Theorem 5.1. *Let U be a fundamental nondegenerate Lucas sequence with parameters P and Q and $p \nmid Q$ be a prime. Then $E_{U,\,p}(x)$ is $O(\log^{p-2} x)$, where the implied constant may depend on p.*

However we cannot resist giving an explicit description of $E_{U,\,p}$ for at least $p = 2$ and $p = 3$ for all cases of $U(P, Q)$.

Theorem 5.2. *Let U be a fundamental nondegenerate Lucas sequence with parameters P and Q with Q odd. Let ρ be the rank of 2 in U. Then for $n \geq 1$*

$$2 \text{ divides } \binom{2n}{n}_U \text{ for all } n \geq 1 \text{ unless } \rho = 3 \text{ and } n = 1.$$

Proof. If $\rho = 3$, then $c_2(n/3, n/3) = 1$ for the same integers as in the Fibonacci case. If $\rho = 2$, then clearly $c_2(n/2, n/2) = 1$ for all $n \geq 1$. □

Theorem 5.3. *Let U be a fundamental nondegenerate Lucas sequence with parameters P and Q, where 3 does not divide Q. Let ρ be the rank of 3 in U. Then for $n \geq 1$*

$$3 \mid \binom{3n}{n}_U \iff \begin{cases} n \neq 3^r \ (r \geq 0), & \text{if } \rho = 2; \\ n \geq 1, & \text{if } \rho = 3; \\ n \neq 1 \text{ and } n \neq 2 \cdot 3^r \ (r \geq 0), & \text{if } \rho = 4. \end{cases}$$

Proof. If ρ is 4, then the analysis is identical to that of the Fibonacci case. If ρ is 3, then it suffices to observe that

$$3 \mid \binom{3n}{n}_U \iff c_3(\frac{n}{3}, \frac{2n}{3}) = 1 \iff c_3(n, 2n) = 1 \iff 3 \mid \binom{3n}{n}.$$

If ρ is 2, then we study $c_3(n/2, n)$. If $n = 2k$, then $c_3(n/2, n) = c_3(k, 2k) = 1$ by Lemma 2.2. If $n = 2k + 1$, then $c_3(n/2, n) = c_3(k, 2k + 1)$. As usual we write $k = \kappa + 3k_1$, $0 \leq \kappa \leq 2$. It is easily checked that $c_3(k, 2k + 1) = 1$ for $\kappa = 0$ or 2. If $\kappa = 1$, then $c_3(k, 2k + 1) = c_3(1 + 3k_1, 3(1 + 2k_1)) = c_3(k_1, 2k_1 + 1)$. In order to have $c_3(k, 2k+1) = 0$, the 3-ary expansion of k must only contain the digit 1, i.e., $k = (3^r - 1)/2$ and $n = 3^r$. □

Remark. That integers of the form 3^r, $r \geq 0$, belong to $E_{U,\,3}$ when P is even, i.e., when $\rho(3) = 2$, will also be a consequence of Theorem 7.1 of Section 7.

6. Question 2 Under the Grill

We now turn to Theorem 1.2 for which a generalization, valid for all primes, not just the prime 3, and all fundamental Lucas sequences, is given.

Theorem 6.1. *Let U be a nondegenerate fundamental Lucas sequence with parameters P and Q. Let p be a prime not dividing Q of rank ρ. Let $s \geq 1$ be an integer. Then p divides $\binom{sn}{n}_U$ for all $n \geq 1$ if and only if the least common multiple of p and ρ divides s, that is,*

$$p \text{ divides } \binom{sn}{n}_U \text{ for all } n \geq 1 \iff \begin{cases} p\rho \mid s, & \text{if } p \nmid D; \\ p \mid s, & \text{if } p \mid D, \end{cases}$$

where $D = P^2 - 4Q$.

Proof. Assume p divides $\binom{sn}{n}_U$ for all $n \geq 1$. For $n = 1$, $\binom{sn}{n}_U = U_s$. But $p \mid U_s$ implies that $\rho \mid s$. Now for all $n \geq 1$ we have

$$\binom{sn}{n}_U = \frac{U_{sn}}{U_n}\binom{sn-1}{n-1}_U. \tag{6.1}$$

Choose $n = \rho$. We assume first p odd and show that $\binom{s\rho-1}{\rho-1}_U$ is not a multiple of p. By the addition formula $2U_{m+n} = V_m U_n + U_m V_n$, we find that

$$2^{\rho-1}\prod_{t=1}^{\rho-1} U_{(s-1)\rho+t} = \prod_{t=1}^{\rho-1}(V_{(s-1)\rho}U_t + U_{(s-1)\rho}V_t) \equiv V_{(s-1)\rho}^{\rho-1} \times \prod_{t=1}^{\rho-1} U_t \pmod{p}.$$

Therefore,

$$\binom{s\rho-1}{\rho-1}_U = \frac{\prod_{t=1}^{\rho-1} U_{(s-1)\rho+t}}{\prod_{t=1}^{\rho-1} U_t} \equiv \left(\frac{V_{(s-1)\rho}}{2}\right)^{\rho-1} \pmod{p}.$$

But $V_{(s-1)\rho}^2 = DU_{(s-1)\rho}^2 + 4Q^{(s-1)\rho} \equiv 4Q^{(s-1)\rho} \pmod{p}$, so $V_{(s-1)\rho} \not\equiv 0 \pmod{p}$. Hence, p divides $U_{s\rho}/U_\rho$. By the law of appearance of prime powers (4.4), p must divide s. Assume now $p = 2$, and $\rho = 3$ since there is nothing more to prove in the case $\rho = 2$. By Theorem 4.2, $2 \mid \binom{3s}{3}_U$ if and only if $c_2(s-1, 1) = 1$. That is, $s-1$ must be odd, and thus s even. Therefore, in all cases, the least common multiple of p and ρ divides s.

Let us prove the converse. Suppose $p \mid D$, i.e., $\rho = p$. Our hypothesis is that $p \mid s$. If $p \nmid n$, then $\nu_p(U_n) = 0$ while $\nu_p(U_{sn}) \geq \nu_p(U_p) \geq 1$. If $p \mid n$, then $\nu_p(U_{sn}) \geq \nu_p(U_{pn}) = 1 + \nu_p(U_n)$. If p is odd, $\nu_p(U_{pn}) = 1 + \nu_p(U_n)$ by (4.4). If $p = 2$, as $P = U_2$ is even by hypothesis, $\nu_p(U_{2n}) = 1 + \nu_p(U_n)$ by Theorem 4.1. Thus, in all cases, p divides U_{sn}/U_n, and $\binom{sn}{n}_U$ by (6.1). Suppose now $p \nmid D$, so p and ρ are coprime and $p\rho \mid s$. Then, for all $n \geq 1$,

$$\nu_p(U_{sn}) \geq \nu_p(U_{p\rho n}) \geq 1 + \nu_p(U_{\rho n}) \geq 1 + \nu_p(U_n),$$

where the inequality $\nu_p(U_{p\rho n}) \geq 1 + \nu_p(U_{\rho n})$ is an equality in all cases unless p is 2, $Q \equiv -1 \pmod 4$ and n is odd, by (4.4) and Theorem 4.1. Hence, again, U_{sn}/U_n is a multiple of p and, by (6.1), $\binom{sn}{n}_U$ is a multiple of p. □

Remark. Propositions 1.5 and 1.6 are also corollaries of Theorem 6.1.

7. The Answer to Question 3

We establish a theorem which generalizes Theorems 1.3 and 2.1 to all nondegenerate fundamental Lucas sequences. Additionally it provides the p-adic valuation of the coefficients $\binom{p^{a+1}}{p^a}_U$ as well as that of the coefficients $\binom{p^b}{p^a}_U$ $(b > a \geq 0)$.

Theorem 7.1. *Let $U = U(P, Q)$ be a nondegenerate fundamental Lucas sequence. Let a and b be two integers with $0 \leq a < b$ and $p \nmid Q$ a prime of rank ρ in U. Then $\nu_p\binom{p^b}{p^a}_U$ equals*

- 0, *if $\rho \mid p-1$, or if $\rho \mid p+1$ and $b-a$ is even;*
- $\begin{cases} b-a, & \text{if } a \geq 1, \\ b-1+\nu_p(U_p), & \text{if } a = 0, \end{cases}$ *if $\rho = p$;*
- $\begin{cases} \nu_p(U_\rho) + \frac{a-1}{2}, & \text{if } a \text{ is odd}, \\ \frac{a}{2} + \delta_2, & \text{if } a \text{ is even}, \end{cases}$ *if $\rho \geq 3$, $\rho \mid p+1$ and $b-a$ is odd,*

where

$$\delta_2 = \begin{cases} 0, & \text{if } p \text{ is odd or } a = 0; \\ \nu_2(P^2 - 3Q) - 1, & \text{if } p \text{ is } 2 \text{ and } a \geq 2. \end{cases}$$

Proof. If $\rho \mid p-1$, then the argument of Theorem 2.1 nearly carries over (no pun intended). That is, if $p - 1 = \sigma\rho$, then

$$\begin{aligned} \frac{p^b}{\rho} - \frac{p^a}{\rho} = \frac{p^a}{\rho}(p^{b-a} - 1) &= \frac{p-1}{\rho} p^a (1 + p + \cdots + p^{b-a-1}) \\ &= \sigma(p^{b-1} + p^{b-2} + \cdots + p^a), \end{aligned}$$

whereas $p^a/\rho < p^a$. Thus, there is no carry in the base-p addition of $(p^b - p^a)/\rho$ and p^a/ρ.

We note here that when adding in base p two nonnegative reals, say x and y, there is a carry at a given position if and only if there is a carry at the same position when subtracting x from $x + y$. (Indeed, $\{x'\} + \{y'\} \geq 1$ if and only if $\{x' + y'\} - \{x'\} < 0$, where x' and y' are any two reals obtained by shifting i places the radix point in the p-ary expansions of both x and y).

If ρ is p, then subtracting p^{a-1} from p^{b-1} in base p produces exactly $b - a$ carries. The first of these carries will occur across the radix point only for $a = 0$. Thus, by Theorem 4.2, the result holds.

Suppose $\rho \mid p + 1$ and $\rho > 2$. Write $\rho\sigma = p + 1$. Note that $1 \leq \sigma < p$. Then the p-adic valuation of $\binom{p^b}{p^a}_U$ depends on relevant carries when subtracting p^a/ρ from p^b/ρ. Now

$$\begin{aligned} \frac{p^b}{\rho} &= \sigma \frac{p^b}{p+1} = \sigma \frac{p^{b-1}}{1 + \frac{1}{p}} \\ &= \sigma(p^{b-1} - p^{b-2} + p^{b-3} - p^{b-4} + \cdots) \\ &= (\sigma - 1)p^{b-1} + (p - \sigma)p^{b-2} + \cdots + d_{a-1}p^{a-1} + (p - 1 - d_{a-1})p^{a-2} + \cdots, \end{aligned}$$

and thus,

$$\frac{p^a}{\rho} = (\sigma - 1)p^{a-1} + (p - \sigma)p^{a-2} + (\sigma - 1)p^{a-3} + (p - \sigma)p^{a-4} + \cdots,$$

where

$$d_{a-1} = \begin{cases} \sigma - 1, & \text{if } b - a \text{ is even;} \\ p - \sigma, & \text{if } b - a \text{ is odd.} \end{cases}$$

Since $\rho = \frac{p+1}{\sigma} > 2$, we see that $p - \sigma > \sigma - 1$. Hence, if $b - a$ is even, then $d_{a-1} = \sigma - 1$ and the subtraction of p^a/ρ from p^b/ρ produces no carry at all. If $b - a$ is odd, then $d_{a-1} = p - \sigma$ and the rightmost relevant carry in subtracting p^a/ρ from p^b/ρ stems from subtraction at position $a - 2$. Subsequent ones occur every two positions till we hit either position 0 or position -1, according to the parity, respectively even or odd, of a. Thus, there are no relevant carries if $a = 0$. The result then follows by application of Theorem 4.2. Note that there is no contradiction between Theorem 4.2 and this theorem for $p = 2$, $\rho = 3$ and a even ≥ 2, when we add δ_2 regardless of the parity of P and the value of $Q \pmod 4$. Indeed, $\rho = 3$ implies P is odd, since $U_2 = P$. However, if P is odd and if $Q \equiv 1 \pmod 4$, then $P^2 - 3Q \equiv 2 \pmod 4$ and so $\delta_2 = 0$. □

We state a simple but striking corollary of Theorem 7.1.

Corollary 7.2. *Let $U(P,Q)$ be a nondegenerate fundamental Lucas sequence where $D = P^2 - 4Q$ is not a square integer. Suppose $p \nmid PQD$ is prime. Then*

$$p \text{ divides } \binom{p^2}{p}_U \quad \text{if and only if} \quad p \text{ is inert in } \mathbb{Q}(\sqrt{D}\,).$$

(To see that the above corollary holds for $p = 2$, we recall that if D is an odd integer, then 2 is inert in $\mathbb{Q}(\sqrt{D}\,)$ if and only if $D \equiv 5 \pmod 8$.)

8. Acknowledgments

We thank an anonymous referee for a careful and useful reading and kind words of praise, and Sana Saadouli for her presence in Caen in the fall of 2014 and her interest in this subject.

References

[1] C. Ballot, *The congruence of Wolstenholme for generalized binomial coefficients related to Lucas sequences*, J. Integer Seq., **18** (2015), Article 15.5.4.
[2] C. Ballot, *Lucas sequences with cyclotomic root field*, Dissertationes Math., **490** (2013), 92 pp.
[3] D. Knuth and H. Wilf, *The power of a prime that divides a generalized binomial coefficient*, J. Reine Angew. Math., **396** (1989), 212–219.
[4] E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math., **44** (1852), 93–146.
[5] D. Marques and P. Trojovský, *On divisibility of Fibonomial coefficients by* 3, J. Integer Seq., **15** (2012), Article 12.6.4.
[6] D. Marques, J. A. Sellers, and P. Trojovský, *On divisibility properties of certain Fibonomial coefficients by a prime*, The Fibonacci Quarterly, **51.1** (2013), 78–83.
[7] M. Ward, *Note on divisibility sequences*, Bull. Amer. Math. Soc., **42.12** (1936), 843–845.

MSC2010: 11B39, 11B65, 11A63

Université de Caen, Département de Mathématiques et Mécanique, F14032 Caen Cedex, France
E-mail address: christian.ballot@unicaen.fr